PATENT
81942.0002
Express Mail Label No. EL 589 806 142 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Masao KASAHARA et al.

Serial No: Not assigned

Filed: November 1, 2000

For: ENCRYPTION METHOD, CRYPTOGRAPHIC COMMUNICATION METHOD, CIPHERTEXT GENERATING DEVICE AND CRYPTOGRAPHIC COMMUNICATION SYSTEM OF PUBLIC-KEY CRYPTOSYSTEM

Art Unit: Not assigned

Examiner: Not assigned

#3

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith are certified copies of Japanese patent application Nos. 11-314371 filed November 4, 1999 and 11-314372 filed November 4, 1999, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: November 1, 2000

By: _____

Louis A. Mok
Registration No. 22,585
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed this Office.

出願年月日
Date of Application: １９９９年１１月 ４日

出願番号
Application Number: 平成１１年特許願第３１４３７１号

出願人
Applicant (s): 村田機械株式会社
笠原 正雄

CERTIFIED COPY OF PRIORITY DOCUMENT

２０００年 ８月１８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０６４８３４

【書類名】　特許願

【整理番号】　20683

【提出日】　平成11年11月 4日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/14

H04L 9/30

G09C 1/00

【発明の名称】　暗号化方法，暗号通信方法及び暗号文作成装置

【請求項の数】　3

【発明者】

【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号

【氏名】　笠原　正雄

【発明者】

【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内

【氏名】　村上　恭通

【特許出願人】

【識別番号】　000006297

【氏名又は名称】　村田機械株式会社

【代表者】　村田　純一

【特許出願人】

【識別番号】　597008636

【氏名又は名称】　笠原　正雄

【代理人】

【識別番号】　100078868

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　06-6944-4141

【手数料の表示】

【予納台帳番号】　001889

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9805283

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化方法，暗号通信方法及び暗号文作成装置

【特許請求の範囲】

【請求項１】　暗号化すべき平文を分割した分割平文と、該分割平文毎に準備してある複数の公開鍵から選択した公開鍵とに基づき暗号文を作成する暗号化方法において、暗号化すべき平文を各ｓビット（ｓ：自然数）の複数の分割平文に分割し、各分割平文毎に準備してある、乱数項が組み込まれた2^s個の公開鍵から各１個の公開鍵を各分割平文毎に自身のビットデータに応じて選択し、選択した公開鍵を使用して暗号文を作成することを特徴とする暗号化方法。

【請求項２】　一方のエンティティ側で平文を分割した分割平文と公開鍵とに基づいて暗号文を作成して他方のエンティティ側へ伝送し、伝送された暗号文を該他方のエンティティ側で元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、暗号化すべき平文を各ｓビット（ｓ：自然数）の複数の分割平文に分割し、各分割平文毎に準備してある、乱数項が組み込まれた2^s個の公開鍵から各１個の公開鍵を各分割平文毎に自身のビットデータに応じて選択し、選択した公開鍵を使用して暗号文を作成し、作成した暗号文を伝送することを特徴とする暗号通信方法。

【請求項３】　暗号化すべき平文を分割した分割平文と公開鍵とに基づいて暗号文を作成する装置において、乱数項が組み込まれた各2^s（ｓ：自然数）個ずつの公開鍵を各分割平文毎に予め格納しておく手段と、暗号化すべき平文を各ｓビットの複数の分割平文に分割する手段と、分割された各分割平文毎に自身のビットデータに応じて前記2^s個の公開鍵から各１個の公開鍵を選択する手段と、選択した公開鍵を使用して暗号文を作成する手段とを備えることを特徴とする暗号文作成装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、公開鍵を用いて平文を暗号文に変換する公開鍵暗号系の暗号化方法、この暗号化方法を利用した暗号通信方法、及び、その暗号文を作成する暗号文

作成装置に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

【０００５】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開さ

れている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

【０００６】

【発明が解決しようとする課題】

公開鍵暗号系の１つの方式として、積和型暗号方式が知られている。これは、送信者である一方のエンティティ側で平文をＫ分割した平文ベクトルｍ＝（m_1，m_2，・・・，m_K）と公開鍵である基数ベクトルｃ＝（c_1，c_2，・・・，c_K）とを用いて、暗号文Ｃ＝m_1 c_1 ＋m_2 c_2 ＋・・・＋m_K c_K を作成し、受信者である他方のエンティティ側でその暗号文Ｃを秘密鍵を用いて平文ベクトルｍに復号して元の平文を得る暗号化方式である。

【０００７】

このような整数環上の演算を利用した積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。そこで、本発明者等は、平文を多進法を用いて表現するようにして、高速な復号処理を可能とした積和型暗号における暗号化方法及び復号方法を提案している（特願平10－262036号，特願平10－262037号）。

【０００８】

以下、特願平10－262036号に提案した暗号化方法及び復号方法について説明する。秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：｛b_i｝，｛v_i｝，Ｐ，ｗ

・公開鍵：｛c_i｝

基数積b_1 b_2 …b_i に乱数項v_i を乗じて、基数B_i を下記（１）のように与える。

$$B_i = v_i\ b_1\ b_2 \cdots b_i \qquad \cdots (1)$$

ここで、式（１）で示される各B_i がほぼ同じ大きさになるようにv_i を設定する。但し、ｇｃｄ（v_i，b_{i+1}）＝１を満たすものとする。

【０００９】

乱数ｗを用いて、公開鍵｛c_i｝を下記（２）のように求める。

$$c_i \equiv w B_i \pmod{P} \quad \cdots (2)$$

平文をＫ分割したメッセージ｛m_i｝と公開鍵｛c_i｝との積和演算により、下記（３）のように、暗号文Ｃを得る。

$$C = m_1 c_1 + m_2 c_2 + \cdots + m_K c_K \quad \cdots (3)$$

【００１０】

復号処理は、以下のようにして行われる。

暗号文Ｃに対して、中間復号文Ｍを下記（４）のようにして求める。

$$M \equiv w^{-1} C \pmod{P} \quad \cdots (4)$$

この中間復号文Ｍは、具体的には式（５）として与えられるので、以下に示す逐次復号アルゴリズムによって復号できる。

$$M = m_1 b_1 v_1 + m_2 b_1 b_2 v_2 + \cdots + m_K b_1 b_2 \cdots b_K v_K \quad \cdots (5)$$

【００１１】

〔逐次復号アルゴリズム〕

ステップ１

$$M_1 = M / b_1$$

$$m_1 \equiv M_1 v_1^{-1} \pmod{b_2}$$

ステップｉ（ｉ＝２～Ｋ－１）

$$M_i = (M_{i-1} - m_{i-1} v_{i-1}) / b_i$$

$$m_i \equiv M_i v_i^{-1} \pmod{b_{i+1}}$$

ステップＫ

$$M_K = (M_{K-1} - m_{K-1} v_{K-1}) / b_K$$

$$m_K = M_K / v_K$$

【００１２】

元来、このような公開鍵暗号方式は、その安全性の根拠を、因数分解の困難さ，離散対数問題を解くことの困難さに置いており、それに対する攻撃も種々のものが提案されている。

【００１３】

また、本発明者等は、圧倒的多数の公開鍵の組合せの中から公開鍵の組を自由に選ぶことができる点に安全性の根拠を置いた新しいタイプの公開鍵暗号系の暗号化方法を提案している（特願平11－269407号）。この方式は、前述した特願平10－262036号提案の方式の改良方式であり、整数と乱数項との積からなる複数の公開鍵が平文を分割した分割平文毎に予め準備されており、準備されているそれらの複数の公開鍵から任意の公開鍵を各分割平文毎に選択し、選択した公開鍵を使用して暗号文を作成するようにしたものである。以下、この特願平11－269407号に提案した暗号化方法及び復号方法について説明する。

【００１４】

特願平10－262036号提案の方式に基づく特願平11－269407号提案の暗号化方式の初回伝送時における中間復号文Mは、下記（６）で与えられる。

$$M = m_1' \, b_1 \, v_1 + m_2' \, b_1 \, b_2 \, v_2 + \cdots + m_K' \, b_1 \, b_2 \cdots b_K \, v_K \qquad \cdots (6)$$

【００１５】

但し、m_i'はメッセージ（分割平文）m_iに対し、$\log_2$ Ｊビットの冗長を付加することにより、与えられたｊについてＪを法として、下記（７）が成立するように符号化されて、各分割平文毎に後述する複数の公開鍵の何れが選択されたかについての情報が伝えられる。

$$m_i' \equiv j \pmod{J} \qquad \cdots (7)$$

【００１６】

図４は、各分割平文毎に予め準備されている複数の公開鍵を示す公開鍵リストを示す図である。図４において、Ｋは平文の分割数（クラス数）を表す。基数積に乱数項を乗じた集合$\{b_1 \, b_2 \cdots b_i \, v_i^{(j)}\}$が、図４に示すように、各分割平文毎（各クラス毎）にＪ個ずつの公開鍵として準備されている。

【００１７】

受信側のエンティティは、基数積と乱数項とのこれらの積を乱数ｗにより変換して公開する。即ち、図４に示す基数積と乱数項との積を下記（８）のように変換し、その集合$\{c_{ij}\}$を公開する。

$$b_1\ b_2 \cdots b_i\ v_i^{(j)}\ w \equiv c_{ij} \pmod{P} \quad \cdots (8)$$

送信側のエンティティがランダムに選択した公開鍵の組を下記（９）と表記する。この場合、送信側のエンティティにとって、J^K （≫１）通りの公開鍵選択の可能性がある。

【００１８】

【数１】

$$(c_{1,j_1}, c_{2,j_2}, \cdots, c_{K,j_K}) \quad \cdots (9)$$

【００１９】

送信側のエンティティは、上記（９）に示す選択した公開鍵の組に基づいて、$m_i' \equiv j_i \pmod{J}$ とした上で、受信側のエンティティへの暗号文Ｃを下記（10）のように生成する。

【００２０】

【数２】

$$C = m_1' c_{1,j_1} + m_2' c_{2,j_2} + \cdots + m_K' c_{K,j_K} \quad \cdots (10)$$

【００２１】

受信側のエンティティは、このようにして生成される暗号文Ｃを復号するために、図４における乱数項 $v_i^{(j)}$ を下記（11）のように予め定めておく。但し、$w_{b,i}$，$r_i^{(j)}$ は何れも乱数である。

$$v_i^{(j)} = w_{b,i} + r_i^{(j)}\ b_{i+1} \quad \cdots (11)$$

更に受信側のエンティティは、下記（12）を満たす $w_{b,i}^{-1}$ を秘密鍵として保持する。

$$w_{b,i} \cdot w_{b,i}^{-1} \equiv 1 \pmod{b_{i+1}} \quad \cdots (12)$$

【００２２】

受信側のエンティティにおける復号処理は、以下のように行われる。中間復号

文M_0は、下記（13）のように与えられる。

【００２３】

【数３】

$$M_0 = m_1' b_1\ v_1^{(j_1)} + m_2' b_1\ b_2\ v_2^{(j_2)} + \cdots$$

$$+ m_K' b_1\ b_2, \cdots b_K\ v_K^{(j_K)} \quad \cdots (13)$$

【００２４】

よって、下記（14）に示す逐次復号アルゴリズムによって復号できる。なお、以下においてb_{K+1}は$m_K' < b_{K+1}$を満たす乱数であるが、基数としては用いられていない。一般にステップｉにおけるj_iに対する乱数項は下記（15）のように表記している。

【００２５】

【数４】

逐次復号アルゴリズム

$$
\left.
\begin{aligned}
&\text{ステップ1} \\
&M_1 = \frac{M_0}{b_1} \\
&m_1' \equiv M_1 \cdot w_{b,1}^{-1} \pmod{b_2} \\
&m_1' \equiv j_1 \pmod{J} \\
&\text{ステップ } i \ (i=2\sim K-1) \\
&M_i = \frac{M_{i-1} - m_{i-1}' v_{i-1}^{(j_{i-1})}}{b_i} \\
&m_i' \equiv M_i w_{b,i}^{-1} \pmod{b_{i+1}} \\
&m_i' \equiv j_i \pmod{J} \\
&\text{ステップK} \\
&M_K = \frac{M_{K-1} - m_{K-1}' v_{K-1}^{(j_{K-1})}}{b_K} \\
&m_K' \equiv M_i w_{b,K}^{-1} \pmod{b_{K+1}}
\end{aligned}
\right\} \cdots (14)
$$

$$
v^{(j_i)} \cdots (15)
$$

【００２６】

上述した特願平11－269407号に提案した暗号化方法は、公開鍵を任意に選択するので、つまり、送信者であるエンティティ側で自由に公開鍵を選択して暗号文を作成するので、その公開鍵の選択パターンが攻撃者には不明であるため、攻撃は困難となる。そして、本発明者等は実用性に富む暗号化方法を更に研究してい

る。

【００２７】

本発明は斯かる事情に鑑みてなされたものであり、公開鍵の自由な選択による安全性は確保しつつ、しかも高速な処理が可能である公開鍵暗号系の加算型による暗号化方法、この暗号化方法を利用した暗号通信方法、及び、その暗号文を作成する暗号文作成装置を提供することを目的とする。

【００２８】

【課題を解決するための手段】

請求項１に係る暗号化方法は、暗号化すべき平文を分割した分割平文と、該分割平文毎に準備してある複数の公開鍵から選択した公開鍵とに基づき暗号文を作成する暗号化方法において、暗号化すべき平文を各ｓビット（ｓ：自然数）の複数の分割平文に分割し、各分割平文毎に準備してある、乱数項が組み込まれた2^s個の公開鍵から各１個の公開鍵を各分割平文毎に自身のビットデータに応じて選択し、選択した公開鍵を使用して暗号文を作成することを特徴とする。

【００２９】

請求項２に係る暗号通信方法は、一方のエンティティ側で平文を分割した分割平文と公開鍵とに基づいて暗号文を作成して他方のエンティティ側へ伝送し、伝送された暗号文を該他方のエンティティ側で元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、暗号化すべき平文を各ｓビット（ｓ：自然数）の複数の分割平文に分割し、各分割平文毎に準備してある、乱数項が組み込まれた2^s個の公開鍵から各１個の公開鍵を各分割平文毎に自身のビットデータに応じて選択し、選択した公開鍵を使用して暗号文を作成し、作成した暗号文を伝送することを特徴とする。

【００３０】

請求項３に係る暗号文作成装置は、暗号化すべき平文を分割した分割平文と公開鍵とに基づいて暗号文を作成する装置において、乱数項が組み込まれた各2^s（ｓ：自然数）個ずつの公開鍵を各分割平文毎に予め格納しておく手段と、暗号化すべき平文を各ｓビットの複数の分割平文に分割する手段と、分割された各分割平文毎に自身のビットデータに応じて前記2^s個の公開鍵から各１個の公開鍵

を選択する手段と、選択した公開鍵を使用して暗号文を作成する手段とを備えることを特徴とする。

【００３１】

本発明では、乱数項が組み込まれた2^s個ずつの公開鍵を各分割平文毎に予め準備しておき、暗号化すべき平文を各ｓビットの複数の分割平文に分割し、各分割平文毎に準備しておいた2^s個の公開鍵から１個の公開鍵を、各分割平文自身のビットデータに応じて選択し、選択した公開鍵を使用して暗号文を作成する。例えばｓ＝１とした場合、乱数項が組み込まれた２個ずつの公開鍵（上下２段ずつ公開鍵リスト）が各分割平文毎に準備されており、各分割平文のビットデータ（”０”，”１”）に応じて何れか一方の公開鍵を選択し、選択した全ての公開鍵を加算して暗号文を作成する。この際、一例として分割平文が”０”である場合には上段の公開鍵を選択し、分割平文が”１”である場合には下段の公開鍵を選択する。本発明では、ビットデータに応じて選択した、乱数項が組み込まれた公開鍵を加算して暗号文を作成するだけであり、暗号化時及び復号時の処理は、極めて速くなる。公開鍵選択の基準とな各分割平文のビットデータは、攻撃者には不明であり、公開鍵の選択パターンが判明することはなく、安全性が高い。

【００３２】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、本発明による暗号化方式をエンティティＡ，Ｂ間の情報通信に利用した状態を示す模式図である。図１の例では、一方のエンティティＡ側で、平文Ｘを暗号文Ｃに暗号化し、通信路１を介してその暗号文Ｃを他方のエンティティＢへ送信し、エンティティＢ側で、その暗号文Ｃを元の平文Ｘに復号する場合を示している。

【００３３】

送信側であるエンティティＡには、平文Ｘを複数の分割平文に分割する平文分割器２と、公開鍵リストを格納するデータベース10から各分割平文に対する公開鍵を選択する公開鍵選択器３と、選択した公開鍵を用いて暗号文Ｃを作成する暗号化器４とが備えられている。また、受信側であるエンティティＢには、送られ

てきた暗号文Ｃを元の平文Ｘに復号する復号器５が備えられている。この例では、公開鍵リストの発行者は受信側のエンティティＢであり、その公開鍵リストの利用者は送信側のエンティティＡである。

【００３４】

次に、具体的な手法について説明する。図２は、各分割平文毎に複数の公開鍵を予め格納しているデータベース10内の公開鍵リストを示す図である。各分割平文毎の公開鍵を（w_1，P_1）によるモジュラー変換で構成すると考えた場合の公開鍵リストを図２に示す。図２において、Ｋは平文Ｘの分割数（クラス数）を表しており、乱数項が組み込まれた２個（上段，下段）ずつの公開鍵がＫ個の各分割平文毎（各クラス毎）に準備されている。なお、図２における乱数$v_i^{(0)}$及び乱数$v_i^{(1)}$は夫々、下記（16）及び（17）を満たす。

$$v_i^{(0)} \equiv 0 \pmod 2 \quad \cdots (16)$$

$$v_i^{(1)} \equiv 1 \pmod 2 \quad \cdots (17)$$

【００３５】

エンティティＡは、平文Ｘを各１ビットのＫ個の分割平文に分割した後、その各分割平文のビットデータに応じて公開鍵を選択する。つまり、分割平文がm_i＝０である場合には上段の公開鍵即ち基数積$2^{i-1} v_i^{(0)}$を選択し、分割平文がm_i＝１である場合には下段の公開鍵即ち基数積$2^{i-1} v_i^{(1)}$を選択し、選択したものを逐次的に加算することにより、エンティティＢへの暗号文Ｃを下記（18）のように作成する。

$$C = v_1^{(t1)} w_1 + 2 v_2^{(t2)} w_1 + \cdots + 2^{K-1} v_K^{(tK)} w_1 \quad \cdots (18)$$

（t1，t2，・・・，tK＝０または１）

【００３６】

例えば、分割平文が（m_1，m_2，m_3，m_4，m_5）＝（０，１，０，１，０）である場合、エンティティＢへの暗号文Ｃは下記（19）のように作成される。

$$C = v_1^{(0)} w_1 + 2 v_2^{(1)} w_1 + 2^2 v_3^{(0)} w_1 + 2^3 v_4^{(1)} w_1 + 2^4 v_5^{(0)} w_1 \quad \cdots (19)$$

【００３７】

このようにして作成された暗号文Ｃは、通信路１を介してエンティティＡからエンティティＢへ送信される。そしてエンティティＢ側で、その暗号文Ｃが元の平文Ｘに復号される。

【００３８】

エンティティＢにおける復号器５での復号処理は、以下のように行われる。

中間復号文M_1を下記（20）のようにして求める。

$$M_1 \equiv C \cdot w_1^{-1} \pmod{P_1} \quad \cdots (20)$$

【００３９】

ここで、中間復号文M_1は明らかに下記（21）のように表せる。但し、ここでは下記（22）を満たすこととする。

【００４０】

【数５】

$$M_1 = v_1^{(m_1)} + 2\, v_2^{(m_2)} + 2^2\, v_3^{(m_3)} \cdots + 2^{K-1}\, v_K^{(m_K)} \quad \cdots (21)$$

$$\left| 2^{i-1}\, v_i^{(m_1)} \right| \geqq K + 64 \quad \cdots (22)$$

【００４１】

よって、下記（23）に示す復号アルゴリズムによって復号できる。この復号アルゴリズムは極めて単純化されていることが分かる。

【００４２】

【数６】

復号アルゴリズム

$$
\left.
\begin{array}{l}
\text{ステップ1} \\
\quad M_1 \equiv 0 \pmod 2 \text{の場合} \quad m_1 = 0 \quad \text{を復号} \\
\quad M_1 \equiv 1 \pmod 2 \text{の場合} \quad m_1 = 1 \quad \text{を復号} \\
\\
\text{ステップ } i \quad (i = 2 \sim K) \\
\quad M_i = \dfrac{M_{i-1} - v_{i-1}^{(m_{i-1})}}{2} \\
\quad M_i \equiv 0 \pmod 2 \text{の場合} \quad m_i = 0 \quad \text{を復号} \\
\quad M_i \equiv 1 \pmod 2 \text{の場合} \quad m_i = 1 \quad \text{を復号}
\end{array}
\right\} \cdots (23)
$$

【００４３】

図３は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、データベース10に予め格納されている複数の公開鍵から各分割平文毎にそれ自身のビットデータに応じて公開鍵を選択する処理と、選択した公開鍵を用いて暗号文を作成する処理とを含むか、または、このように作成された暗号文を上述した復号アルゴリズムに従って復号する処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ20は、各エンティティ側に設けられている。

【００４４】

図３において、コンピュータ20とオンライン接続する記録媒体21は、コンピュータ20の設置場所から隔たって設置される例えばＷＷＷ(World Wide Web)のサーバコンピュータを用いてなり、記録媒体21には前述の如きプログラム21a が記録されている。記録媒体21から読み出されたプログラム21a がコンピュータ20を制御することにより、コンピュータ20が暗号文Ｃを作成するか、または、暗号文Ｃを元の平文Ｘに復号する。

【００４５】

コンピュータ20の内部に設けられた記録媒体22は、内蔵設置される例えばハードディスクドライブまたはＲＯＭ等を用いてなり、記録媒体22には前述の如きプログラム22a が記録されている。記録媒体22から読み出されたプログラム22a がコンピュータ20を制御することにより、コンピュータ20が暗号文Ｃを作成するか、または、暗号文Ｃを元の平文Ｘに復号する。

【００４６】

コンピュータ20に設けられたディスクドライブ20a に装填して使用される記録媒体23は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスク等を用いてなり、記録媒体23には前述の如きプログラム23a が記録されている。記録媒体23から読み出されたプログラム23a がコンピュータ20を制御することにより、コンピュータ20が暗号文Ｃを作成するか、または、暗号文Ｃを元の平文Ｘに復号する。

【００４７】

以下、本発明の暗号化方式の特徴について、これによく似た０，１ナップザック暗号との対比を中心にして説明する。従来の０，１ナップザック暗号とは、$\Sigma m_i c_i$ という形になっていない点、つまり積和型ではなく加算型であるという点で注目すべき差が存在している。

【００４８】

本発明の方式では、連接平文において重み率＝１／２であり、この意味で連接攻撃に対して強化されていると考えられる。この本発明の方式は、従来の０，１ナップザック暗号と比較して以下のような著しい特徴を有している。

【００４９】

本発明の方式においては、図２の上段に対応する公開鍵（c_1，c_2，・・・，c_K）に基づく下記（24）に示す暗号文Ｃと、図２の下段に対応する公開鍵（c_1'，c_2'，・・・，c_K'）に基づく下記（25）に示す暗号文Ｃ′との和として、暗号文C^Sが下記（26）のように与えられる。

【００５０】

【数７】

$$C = \sum \overline{m_i}\, c_i \quad \cdots (24)$$

$$C' = \sum m_i\, c_i' \quad \cdots (25)$$

$$C^S = C + C' \quad \cdots (26)$$

【００５１】

例えば、分割平文が（m_1，m_2，m_3，m_4，m_5）＝（０，１，１，０，１）である場合、暗号文Ｃ及び暗号文Ｃ′は夫々、下記（27）及び（28）のようになる。

【００５２】

【数８】

$$C = \overline{m_1} c_1 + \overline{m_4} c_4 \quad \cdots (27)$$

$$C' = m_2 c_2' + m_3 c_3' + m_5 c_5' \quad \cdots (28)$$

【００５３】

暗号文Ｃ，Ｃ′は多段暗号化されると共に、夫々の暗号文Ｃ，Ｃ′は異なる乱数｛v_i｝，｛v_i'｝によって安全な方向に工夫されている。本発明の方式の暗号文C^Sが２つの見かけ上異なるナップザック暗号の暗号文の和として与えられており、この意味で０，１ナップザック暗号に１つの突破口が与えられたと考えられる。ＬＬＬ（Lenstra-Lenstra-Lovasz）攻撃に関しては、攻撃側にとって（入力平文長）／（暗号文）≒２であり、その攻撃はかなり困難であると考えられる。

【００５４】

以下、安全性を向上させるようにした本発明の応用例について説明する。

（多段暗号化の適用）

これは、本発明者等が特願平11－173338号に提案した暗号化方法（多段暗号化の概念）を上述した暗号化方法に適用したものであり、分割平文毎に選択した公開鍵に複数の乱数を多段化演算した演算結果を用いて暗号文を作成する。図２の基数積に対し、乱数ｗと素数Ｐとの組（ｗ，Ｐ）を複数組（Ｓ組）設定し、Ｓ段にわたって乱数を乗じていくことにより、最終的に得られるものを公開鍵として利用する。このように、本発明の基本の暗号化方式に多段暗号化手法を適用することにより、安全性をより高くした方式を構築できる。

【００５５】

（積和積暗号化の適用）

これは、本発明者等が特願平11－205381号に提案した暗号化方法（積和積暗号化の概念）を上述した暗号化方法に適用したものであり、選択した複数の公開鍵を加算して得られる加算項を複数設定し、それらの複数の加算項を積及び／または和の形式で結合することにより暗号文を作成する。各分割平文のビットデータに応じて選択した複数の公開鍵を用いて上記（18）に示されるような加算項を複数組作成し、作成したそれらの複数組の加算項同士を更に乗算及び／または加算して暗号文を作成する。このように、本発明の基本の暗号化方式に積和積暗号化手法を適用することにより、安全性をより高くした方式を構築できる。

【００５６】

なお、上述した例では、各分割平文を１ビット、各分割平文毎の選択対象の公開鍵を２個とする場合（ｓ＝１）について説明したが、下記（29）を満たす下記（30）に示すような乱数を用いることにより、$b_i = 2^s$（ｓ：２以上の自然数）の場合に拡張することが可能である。例えば、ｓ＝２である場合には、各分割平文毎に４個ずつの公開鍵が準備されており、平文を各２ビットの分割平文に分割し、各分割平文毎にそのビットデータに応じて４個の公開鍵から１個の公開鍵を選択し、選択した全ての公開鍵を加算した形で暗号文を作成する。

【００５７】

【数９】

$$v_i^{(m_i)} \equiv m \pmod{2^s} \quad \cdots(29)$$

$$v_i^{(m_i)} \quad \cdots(30)$$

【００５８】

なお、上述した例では、暗号通信システムの場合について説明したが、平文を暗号化して暗号文を作成し、作成した暗号文を単に記録するような場合にも、本発明の暗号化方法を適用できることは勿論である。

【００５９】

【発明の効果】

以上詳述したように、本発明では、乱数項が組み込まれた2^s個ずつの公開鍵を各分割平文毎に予め準備しておき、暗号化すべき平文を各ｓビットの複数の分割平文に分割し、各分割平文毎に準備しておいた2^s個の公開鍵から１個の公開鍵を各分割平文毎にそれ自身のビットデータに応じて選択し、選択した公開鍵を使用して暗号文を作成するようにしたので、公開鍵の自由な選択による安全性を確保しながら、高速な暗号化・復号処理が可能となり、公開鍵暗号方式の発展及び実用化を図る上で、本発明は大いに寄与できる。

【００６０】

（付記）

なお、以上の説明に対して更に以下の項を開示する。

（１）　請求項１記載の暗号化方法であって、選択した複数の公開鍵を加算した形式で暗号文を作成する暗号化方法。

（２）　請求項１記載の暗号化方法であって、選択した複数の公開鍵を加算して得られる複数の加算項を更に乗算及び／または加算した形式で暗号文を作成する暗号化方法。

（３）　請求項１記載の暗号化方法であって、選択した公開鍵に複数の乱数を多

段化演算した演算結果を利用して暗号文を作成する暗号化方法。

（４）　複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１または第（１），（２），（３）項の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文から元の平文を復号する復号器とを備える暗号通信システム。

（５）　請求項１または第（１），（２），（３）項の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を記録する記録器とを備える暗号化・記録装置。

（６）　コンピュータに、暗号化すべき平文を分割した分割平文と公開鍵とに基づいて暗号文を作成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を各ｓビット（ｓ：自然数）の複数の分割平文に分割することをコンピュータに実行させるプログラムコード手段と、各分割平文毎に準備してある、乱数項が組み込まれた2^s個の公開鍵から、各１個の公開鍵を各分割平文毎にそれ自身のビットデータに応じて選択することをコンピュータに実行させるプログラムコード手段と、選択した公開鍵を使用して暗号文を作成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されている記録媒体。

（７）　コンピュータに、平文を分割した各ｓビットの複数の各分割平文毎に準備してある、乱数項が組み込まれた2^s個（ｓ：自然数）の公開鍵から、各分割平文毎にそれ自身のビットデータに応じて１個ずつ選択した複数の公開鍵を用いて作成された暗号文を復号させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体であって、選択された前記公開鍵を同定しながら前記分割平文を順次復号することをコンピュータに実行させるプログラムコード手段を含むプログラムが記録されている記録媒体。

【図面の簡単な説明】

【図１】

２人のエンティティ間における情報の暗号通信状態を示す模式図である。

【図２】

データベース内の公開鍵リストを示す図である。

【図３】

記録媒体の実施の形態の構成を示す図である。

【図４】

特願平11－269407号提案の暗号化方式における公開鍵リストを示す図である。

【符号の説明】

1　通信路

2　平文分割器

3　公開鍵選択器

4　暗号化器

5　復号器

10　データベース

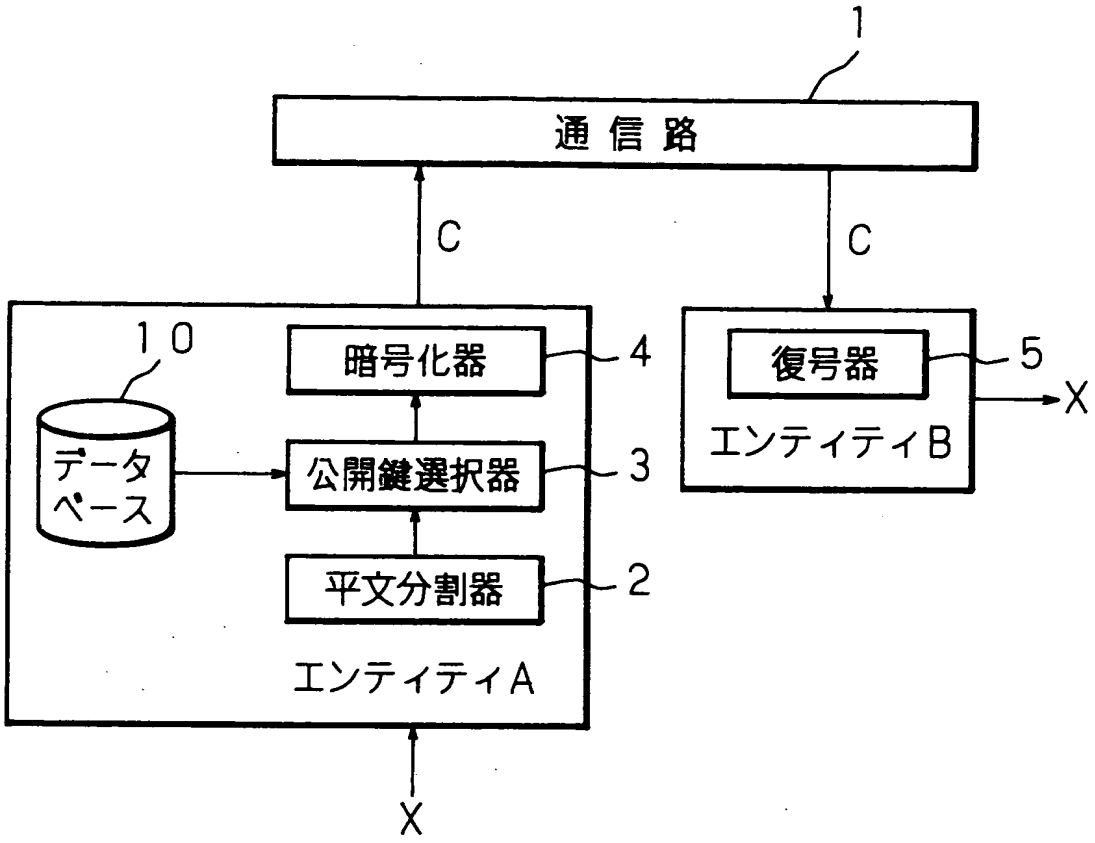
20　コンピュータ

21，22，23　記録媒体

A，B　エンティティ

【書類名】　　図面

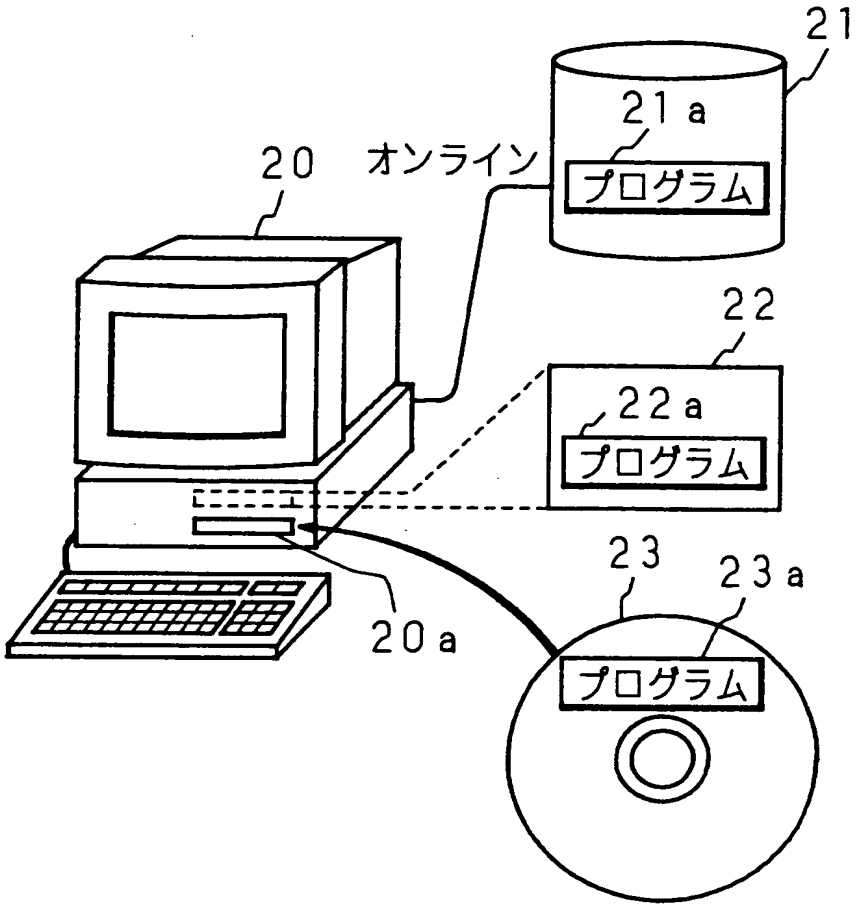
【図１】


1
通信路
C
C
10
データベース
暗号化器
4
公開鍵選択器
3
平文分割器
2
エンティティA
復号器
5
X
エンティティB
X

【図２】

クラス１	クラス２	クラス３	…	クラスＫ
$v_1^{(0)} w_1$	$2 v_2^{(0)} w_1$	$2^2 v_3^{(0)} w_1$	…	$2^{K-1} v_K^{(0)} w_1$
$v_1^{(1)} w_1$	$2 v_2^{(1)} w_1$	$2^2 v_3^{(1)} w_1$	…	$2^{K-1} v_K^{(1)} w_1$

【図３】



【図４】

クラス1	クラス2	…	クラスK
$b_1 v_1^{(1)}$	$b_1 b_2 v_2^{(1)}$	…	$b_1 b_2 \cdots b_K v_K^{(1)}$
$b_1 v_1^{(2)}$	$b_1 b_2 v_2^{(2)}$	…	$b_1 b_2 \cdots b_K v_K^{(2)}$
⋮	⋮		⋮
$b_1 v_1^{(J)}$	$b_1 b_2 v_2^{(J)}$	…	$b_1 b_2 \cdots b_K v_K^{(J)}$

【書類名】　　要約書

【要約】

【課題】　公開鍵の自由な選択による安全性は確保しつつ、しかも高速な処理が可能である公開鍵暗号系の加算型による暗号化方法を提供する。

【解決手段】　乱数項を組み込んだ２個ずつの公開鍵を各分割平文毎に予めデータベース10内に準備しておき、平文Ｘを各１ビットの複数の分割平文に分割し、それ自身のビットデータに応じて各分割平文毎にデータベース10から１個の公開鍵を選択し、選択した公開鍵を加算して暗号文Ｃを作成する。安全性の根拠を、所望の公開鍵の組を自由に選択できることに置いている。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００６２９７〕

１．変更年月日　　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９７００８６３６〕

１．変更年月日　　１９９７年　１月２１日
［変更理由］　新規登録
住　所　　大阪府箕面市粟生外院４丁目１５番３号
氏　名　　笠原　正雄